UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/599,230	09/22/2006	Karl Asperger	78857.105107	6068

86528 7590 04/09/2012

King & Spalding LLP
401 Congress Avenue
Suite 3200
Austin, TX 78701

EXAMINER	
LEE, JASON T	

ART UNIT	PAPER NUMBER
2438	

NOTIFICATION DATE	DELIVERY MODE
04/09/2012	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

AustinUSPTO@kslaw.com
AustinIP@kslaw.com
emitchell@kslaw.com

Office Action Summary	Application No.	Applicant(s)	
	10/599,230	ASPERGER ET AL.	
	Examiner	Art Unit	
	JASON LEE	2438	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *22 February 2012*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

5)☒ Claim(s) *1-6 and 8-21* is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6)☐ Claim(s) _____ is/are allowed.

7)☒ Claim(s) *1-6 and 8-21* is/are rejected.

8)☐ Claim(s) _____ is/are objected to.

9)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

12)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. The following is a final office action in response to applicant's amendment filed on February 22, 2012. Claims 1, 13 and 20 have been amended. Claim 21 has been added. Claim 7 has been cancelled. Therefore, claims 1-6 and 8-21 are pending and addressed below.

Response to Arguments

2. Applicant's amendments are sufficient to overcome the claim rejections the USC 112 second paragraph for claim 13 set forth in the previous office action. Applicant amended the claim 13 to recite "a die of the semiconductor chip" to clarify the claimed limitation. Therefore, the 112 second paragraph rejections for claim 13 has been withdrawn.

3. Applicant's arguments filed on February 22, 2012 with respect to newly amended independent claims 1 and 20 (see Remark page 8-9) have been fully considered. Applicant amended the independent claim 1 to add "monitor an ohmic resistance of at least one electrical line… compare the monitored ohmic resistance of the at least one electrical line with a threshold resistance value, detect a breaking of the electrical line based on the comparison…"; independent claim 20 to add "an integrated voltage regulator that regulates an operating voltage or current of the integrated circuit to render the operating voltage or current noisy to an outside observer, thus preventing attacks based on examination of the current of the integrated circuit" which is not presented any previous listing of the claims. Thus, the scope of the claims has been changed. Accordingly, new ground of rejection is being introduced to address the newly added limitation. Please see below for the new grounds of rejections.

Claim Rejections - 35 USC § 112

4. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

5. Claims 1, 20 and 21 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. For example, Claims 1 recites "compare the monitored ohmic resistance of the at least one electrical line with a threshold resistance value". There is no support by the specification for the limitation of "a threshold resistance value". Nowhere in the cited paragraphs or in the rest of the instant application's specification has the limitation "a threshold resistance value "been taught. Indeed there is no mention about "a threshold resistance value " in the entire specification. For claim 20, it recites "an integrated voltage regulator that regulates an operating voltage or current of the integrated circuit to render the operating voltage or current noisy to an outside observer, thus preventing attacks based on examination of the current of the integrated circuit". There is no support by the specification for the limitation of "an outside observer". Nowhere in the cited paragraphs or in the rest of the instant application's specification has the limitation "an outside observer" been taught. For newly added claim 21, it recites "a particular state of the protective layer". There is no mention of "a particular state of the protective layer". There is no support by the

specification for the limitation of "a particular state". Therefore, these limitations are considered to introduce new matter.

6. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

7. Newly added Claim 21 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Newly added claim 21 recites "a particular state of the protective layer". It is not clear for what "a particular state" means. There is no description in the instant Specification for what "a particular state" means. For an ordinary skill in the art, it is difficult to what "particular" state is. Thus, claim 21 renders indefinite.

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9. Claims 1-6, 8-14, 16, 19 and 20-21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kömmerling et al (US 7,005,733 B2) hereinafter Kömmerling, in view of Mizuno et al (WO 03/015169 A1) hereinafter Mizuno.

Examiner notes: Mizuno et al (WO 03/015169 A1) was published in Japanese and published in 2/20/2003. For translation purposes, citation are made based on US

2004/0212017 A1, which is an US equivalent for the WIPO (WO 03/015169 A1) publication.

As for claim 1:

Kömmerling discloses **an integrated circuit** (See Kömmerling Fig 1A) **comprising function modules, wherein the function modules comprise: a central processing unit designed to process data and to execute programs,** (See Kömmerling column 5 lines 33-34 "The apparatus of FIG. 1A comprises a central processing unit (CPU) 100, which might be a standard CPU core") **a cache memory,** (See Kömmerling column 5 lines 36-37 " The apparatus further comprises a non-volatile (NV) memory 110") **an encryption unit designed to encrypt and decrypt data** (See Kömmerling column 5 lines 45-50 " The encryption/decryption unit 120 operates to encrypt and decrypt using an encryption key 160 provided from a cryptographic input unit 130. The cryptographic input unit 130 is operative to form the key 160 from a plurality of detected property outputs 140 of a corresponding plurality of sensors 150 which are responsive to the encapsulation properties 170 of an encapsulation 50 surrounding the circuit.") **and a security sensor system including a protective layer on the integrated circuit including at least one elongated electrical line extending along the surface of the integrated circuit, the security sensor system operable to:** (See Kömmerling column 11 lines 28-49 "It is thus possible in this embodiment to measure the resistance in a path through the encapsulation 50 between any pair of the sensors. Since the resistivity of the encapsulation varies due to the distribution of the particles 385, each such resistance will be different. Because the current flows across the device through

the encapsulation, any hole between sensors will change the current flowing and will alter the readings. The sensor output reading for each point in this case may conveniently be calculated as the sum of the currents measured as flowing into each of it's neighbours from the sensor, so that a point on the substrate (and the encapsulation above it) will lie within the areas to which several sensors are responsive") **monitor an ohmic resistance of at least one electrical line of the protective layer on the integrated circuit, compare the monitored ohmic resistance of the at least one electrical line with a threshold resistance value, detect a breaking of the electrical line based on the comparison, and when a breaking of the electrical line is detected, automatically initiate the deletion of data from at least one memory of the integrated circuit.** (See Kömmerling column 3 lines 46-56 "embodiments are effective in protecting the chip against attack when no power is supplied to the chip. To additionally protect the chip in the powered up condition, additional measures may be desirable. For instance, the physical parameter may be scanned from the protective member at relatively frequent intervals (more frequent than the minimum time which would be taken to pierce or remove the protective member). On noting a change in the value, action could be taken to erase the secure content (i.e. encrypted data) held on the chip or otherwise disable the chip, as in the prior art.")

Kömmerling discloses an integrated circuit device with anti-tamper encapsulation, so when tampering with the encapsulation to gain access to the circuit causes the encryption and/or decryption to fail. (See Kömmerling abstract). Kömmerling does not

explicitly disclose the limitation of "**monitor an ohmic resistance of at least one electrical line of the protective layer on the integrated circuit, compare the monitored ohmic resistance of the at least one electrical line with a threshold resistance value, detect a breaking of the electrical line based on the comparison**"; however, Mizuno discloses as claimed (see Mizuno page 15 lines 5-22 for original Japanese description, for translation purposes as stated above, the corresponding translation is equivalent to US 2004/0212017 A1) for [0096] of sixth embodiment "plural processing detector circuits 20 are dispersed irregularly within the main surface of the chip 3, whereby it is possible to make it difficult to identify the positions of the processing detector circuits 20 in the chip 3. In this regard, for analyzing information stored in the chip 3, it is conceivable that, after destroying the processing detector circuits 20, the foregoing wiring lines which function as a shield can be removed, followed by analysis of information stored in the chip 3. Therefore, if plural processing detector circuits 20 are arranged in an irregularly dispersed fashion, it becomes difficult to destroy all of the processing detector circuits, and, hence, it is possible to make the analysis of information difficult. As a result, it becomes possible to further improve the security of information stored in the chip 3. Once the wiring lines 5A and 5B for the supply voltage are subjected to processing (complete or partial cutting), the processing detector circuits 20 are able to detect a change in potential (or resistance) of the wiring lines 5A and 5B. That is, the processing detector circuits 20 are used for the detection of tampering with the wiring lines 5A and 5B.")

Mizuno, similar to Kömmerling, is in the same field of endeavor of anti-tampering for semiconductors device, discloses the resistance change condition as claimed limitation for protection of the breaking of the wiring lines. (See Mizuno abstract)

Therefore, it would have been obvious to one of the ordinary skill in the art to use Mizuno in the invention of Kömmerling to include "the wiring line with detection circuit of resistance of the change and analyze the value of resistance for breaking in semiconductor chip design environment" as taught by Mizuno in order to improve the security of the IC for further protection for the circuit. (See Mizuno [0179-0183])

As for claim 2:

The combination of Kömmerling and Mizuno discloses **the integrated circuit according to claim 1, wherein the function modules comprise a random-number generator.** (See Kömmerling column 16 lines 39-49 "the key management unit 702 comprises a sensor address generator 801, ...The KMU (key management unit) 702 stores a random number as the pairing key, in an erasable register (i.e. non-volatile memory) 824. The random number is unique to each device of a batch and is supplied through the I/O circuit on initialisation and stored in the register by the loader program.")

As for claim 3:

The combination of Kömmerling and Mizuno discloses **the integrated circuit according to claim 1, wherein function modules comprise a first memory in which cryptological keys are stored.** (see Kömmerling column 17 lines 6-21 "the final key to be used is calculated from the contents of the Shell Key Register 804 and the pairing key register 824 using, for example, an XOR combination operation and stored in the

final key register 722 ,,,the key to the ROM, which was initially stored in the clear in register 724, is retrieved and encrypted under the final key from register 722, and stored back in the register 724 in that encrypted form")

As for claim 4:

The combination of Kömmerling and Mizuno discloses **the integrated circuit according to claim 3, wherein cryptological keys which are stored in the first memory are generated by means of the random-number generator.** (See Kömmerling FIG 19 and column 16 lines 39 to column 17 lines 21)

As for claim 5:

The combination of Kömmerling and Mizuno discloses **the integrated circuit according to claim 1**, **wherein function modules comprise a real-time clock.** (See Kömmerling FIG 9 and column 45-50 " the encryption/decryption circuit 120 is supplied in self timed logic, rather than being driven from the CPU clock, so as to be able to operate faster than the CPU and hence to make the encryption/decryption process as fast as the available clock speed on the integrated circuit.") Kömmerling implies the encryption/decryption circuit use a self-timed logic (thus, real-time clock) rather than being driven from the CPU clock.

As for claim 6:

The combination of Kömmerling and Mizuno discloses **the integrated circuit according to claim 1, wherein operating parameters to be monitored additionally is the clock frequency of the real-time clock and/or an operating temperature at a point in the integrated circuit and/or an operating voltage of the integrated circuit.**

(See Kömmerling column 9 lines 25-30 "The ADC output is then corrected by a tolerance compensation circuit 320, responsive for example to a thermistor or other temperature sensor (not shown), to correct each digital sensor reading for the effect of temperature (or other environment factors) in accordance with some predetermined correction scale.")

As for claim 8:

The combination of Kömmerling and Mizuno discloses **the integrated circuit according to claim 1, wherein it is arranged in a package and has terminal contacts brought out of the package.** (See Kömmerling column 5 lines 1-3 "FIG. 12A is a pictorial illustration of a packaged electrical circuit assembly constructed and operative in accordance with an alternative embodiment")

As for claim 9:

The combination of Kömmerling and Mizuno discloses **the integrated circuit according to claim 1, wherein individual function modules have an essentially planar extent and are arranged adjacently to one another in the area of the normal to the surface.** (See Kömmerling FIG 11, and Mizuno Fig 11). There are individual function modules in the planar of the circuit surface that are arranged adjactently to one another.

As for claim 10:

The combination of Kömmerling and Mizuno discloses **the integrated circuit according to claim 1, wherein the function modules comprise an integrated voltage regulator which regulates an operating voltage.** (see Kömmerling column

12 lines 23-25 “such a signal may be obtained by rapidly alternating the sensor 150 between 0 volts and supply voltage level, so as to produce a signal with an alternating component between the sensors 150 and the upper layer 390”) Kömmerling discloses the voltage supply; it is obvious there is voltage regulator for the supply of the voltage.

As for claim 11:

The combination of Kömmerling and Mizuno discloses **the integrated circuit according to claim 1, wherein it is constructed as semiconductor chip.** (See Kömmerling column 2 lines 16-19 “to provide an improved apparatus and method for protecting the content of memories in circuit assemblies (such as integrated circuits, e.g. semiconductor chips)”)

As for claim 12:

The combination of Kömmerling and Mizuno discloses **the integrated circuit according to claim 11, wherein semiconductor structures of the individual function modules are intermeshed in the manner of a puzzle in order to avoid individual function modules from being recognizable.** (see Mizuno FIG 4, 7, and 8 with [0066] " The wiring lines 5A and 5B are formed in the shape of comb teeth as seen in plan view and the respective teeth are arranged so as to mesh with each other in the same wiring layer.”)

Examiner supplies the same rational for the combination of the reference as in claim 1 above.

As for claim 13:

The combination of Kömmerling and Mizuno discloses **the integrated circuit according to claim 11, wherein an active protective layer which consists of at least one elongated electrical line which extends along the surface of a die of the semiconductor chip, particularly in mutually parallel tracks section by section, is applied directly to the die of the semiconductor chip.** (See Mizuno FIG 4 (for parallel tracks) and 6 (for the die of the semiconductor chip)

Examiner supplies the same rational for the combination of the reference as in claim 1 above.

As for claim 14:

The combination of Kömmerling and Mizuno **an arrangement comprising an integrated circuit as claimed claim 1, wherein the integrated circuit is connected by means of a data bus to a second memory in which data are stored encrypted, wherein the second memory has memory cells which in each case have a memory address and each memory cell can be addressed directly in reading or writing manner.** (See Kömmerling column 17 lines 65 to column 18 lines 5 "The decrypted 64 bit word is written by the block encryption unit 260 to the plaintext register 728. In response to the row portion of the address placed on the address bus 712, the memory access control circuit 726 selects the appropriate one of the registers 730a h which contains the byte requested by the CPU 100 and causes the selected register to load that byte onto the data bus 710 for reading by the CPU 100.")

As for claim 16:

The combination of Kömmerling and Mizuno **an arrangement comprising an integrated circuit as claimed claim 1, wherein the integrated circuit is connected by means of a data bus to a non-volatile third memory in which data or program code are stored encrypted.** (See Kömmerling column 15 lines 8-13 "memory 110 is a read only memory (ROM). Data is provided within the read only memory 110 in encrypted form, encrypted using a first predetermined encryption key. The first encryption key is then stored, in the clear, in the second memory 111 which is writeable, non-volatile, memory (e.g. Flash or EEPROM).")

As for claim 19:

The combination of Kömmerling and Mizuno **an arrangement comprising an integrated circuit as claimed claim 16, wherein the third memory is a Flash memory or ROM.** (See column 15 lines 8 "memory 110 is a read only memory (ROM)." And column 5 lines 36-39 "The apparatus further comprises a non-volatile (NV) memory 110 which, in this embodiment, is alterable (it is for example FLASH or EEPROM or ferro electric random access memory (FERAM)).")

As for claim 20:

Kömmerling discloses **an integrated circuit** (See Kömmerling Fig 1A) **comprising function modules, wherein the function modules comprise: a central processing unit designed to process data and to execute programs,** (See Kömmerling column 5 lines 33-34 "The apparatus of FIG. 1A comprises a central processing unit (CPU) 100, which might be a standard CPU core") **a cache memory,** (See Kömmerling column 5 lines 36-37 " The apparatus further comprises a non-volatile (NV) memory 110")

an encryption unit designed to encrypt and decrypt data (See Kömmerling column 5 lines 45-50 " The encryption/decryption unit 120 operates to encrypt and decrypt using an encryption key 160 provided from a cryptographic input unit 130. The cryptographic input unit 130 is operative to form the key 160 from a plurality of detected property outputs 140 of a corresponding plurality of sensors 150 which are responsive to the encapsulation properties 170 of an encapsulation 50 surrounding the circuit.") **and the function modules comprise a security sensor system including a protective layer on the integrated circuit including at least one elongated electrical line extending along the surface of the integrated circuit, the security sensor system operable to monitor the state of the protective layer on the integrated circuit such that when a breaking of the electrical line is detected, data is automatically deleted from at least one memory of the integrated circuit,** (See Kömmerling column 11 lines 28-49 "It is thus possible in this embodiment to measure the resistance in a path through the encapsulation 50 between any pair of the sensors. Since the resistivity of the encapsulation varies due to the distribution of the particles 385, each such resistance will be different. Because the current flows across the device through the encapsulation, any hole between sensors will change the current flowing and will alter the readings. The sensor output reading for each point in this case may conveniently be calculated as the sum of the currents measured as flowing into each of it's neighbours from the sensor, so that a point on the substrate (and the encapsulation above it) will lie within the areas to which several sensors are responsive" and Kömmerling column 3 lines 46-56 "embodiments are effective in protecting the chip

against attack when no power is supplied to the chip. To additionally protect the chip in the powered up condition, additional measures may be desirable. For instance, the physical parameter may be scanned from the protective member at relatively frequent intervals (more frequent than the minimum time which would be taken to pierce or remove the protective member). On noting a change in the value, action could be taken to erase the secure content (i.e. encrypted data) held on the chip or otherwise disable the chip, as in the prior art.") **a random-number generator and a first memory in which cryptological keys are stored, and wherein cryptological keys which are stored in the first memory are generated by means of the random-number generator,** (see Kömmerling column 16 lines 39-49 "the key management unit 702 comprises a sensor address generator 801, ...The KMU (key management unit) 702 stores a random number as the pairing key, in an erasable register (i.e. non-volatile memory) 824. The random number is unique to each device of a batch and is supplied through the I/O circuit on initialisation and stored in the register by the loader program.") **and an integrated voltage regulator that regulates an operating voltage or current of the integrated circuit to render the operating voltage or current noisy to an outside observer, thus preventing attacks based on examination of the current of the integrated circuit.**

Kömmerling discloses an integrated circuit device with anti-tamper encapsulation, so when tampering with the encapsulation to gain access to the circuit causes the encryption and/or decryption to fail. (See Kömmerling abstract). Kömmerling does not explicitly disclose the limitation of "**an integrated voltage regulator that regulates an**

operating voltage or current of the integrated circuit to render the operating voltage or current noisy to an outside observer, thus preventing attacks based on examination of the current of the integrated circuit"; however, Mizuno discloses as claimed (see Mizuno page 15 lines 5-22 for original Japanese description, for translation purposes as stated above, the corresponding translation is equivalent to US 2004/0212017 A1) for [0096] of sixth embodiment "plural processing detector circuits 20 are dispersed irregularly within the main surface of the chip 3, whereby it is possible to make it difficult to identify the positions of the processing detector circuits 20 in the chip 3. In this regard, for analyzing information stored in the chip 3, it is conceivable that, after destroying the processing detector circuits 20, the foregoing wiring lines which function as a shield can be removed, followed by analysis of information stored in the chip 3. Therefore, if plural processing detector circuits 20 are arranged in an irregularly dispersed fashion, it becomes difficult to destroy all of the processing detector circuits, and, hence, it is possible to make the analysis of information difficult. As a result, it becomes possible to further improve the security of information stored in the chip 3. Once the wiring lines 5A and 5B for the supply voltage are subjected to processing (complete or partial cutting), the processing detector circuits 20 are able to detect a change in potential (or resistance) of the wiring lines 5A and 5B. That is, the processing detector circuits 20 are used for the detection of tampering with the wiring lines 5A and 5B.")

Mizuno, similar to Kömmerling, is in the same field of endeavor of anti-tampering for semiconductors device, discloses the resistance change condition as claimed limitation

for protection of the breaking of the wiring lines. (See Mizuno abstract) The analysis of the value of resistance is similar for a voltage regulator for an outside observer to compare the voltage or current.

Therefore, it would have been obvious to one of the ordinary skill in the art to use Mizuno in the invention of Kömmerling to include "the wiring line with detection circuit of resistance of the change and analyze the value of resistance for breaking in semiconductor chip design environment" as taught by Mizuno in order to improve the security of the IC for further protection for the circuit. (See Mizuno [0179-0183])

As for claim 21:

Kömmerling discloses **an integrated circuit** (See Kömmerling Fig 1A) **including:**

an integrated circuit comprising: a central processing unit designed to process data and to execute programs, (See Kömmerling column 5 lines 33-34 "The apparatus of FIG. 1A comprises a central processing unit (CPU) 100, which might be a standard CPU core")

a first memory (See Kömmerling column 5 lines 36-37 " The apparatus further comprises a non-volatile (NV) memory 110") **storing a cryptographic key, an encryption unit designed to encrypt and decrypt data using the cryptographic key stored in the first memory,** (See Kömmerling column 5 lines 45-50 " The encryption/decryption unit 120 operates to encrypt and decrypt using an encryption key 160 provided from a cryptographic input unit 130. The cryptographic input unit 130 is operative to form the key 160 from a plurality of detected property outputs 140 of a corresponding plurality of sensors 150 which are responsive to the encapsulation

properties 170 of an encapsulation 50 surrounding the circuit.") **a security sensor system including a protective layer covering the integrated circuit and a monitoring system that monitors the state of the protective layer covering the integrated circuit such that when a particular state of the protective layer is detected, data is automatically deleted from at least one memory of the integrated circuit,** (See Kömmerling column 3 lines 46-56 "embodiments are effective in protecting the chip against attack when no power is supplied to the chip. To additionally protect the chip in the powered up condition, additional measures may be desirable. For instance, the physical parameter may be scanned from the protective member at relatively frequent intervals (more frequent than the minimum time which would be taken to pierce or remove the protective member). On noting a change in the value, action could be taken to erase the secure content (i.e. encrypted data) held on the chip or otherwise disable the chip, as in the prior art.") **and at least one terminal contact extending through the protective layer covering the integrated circuit, and an external second memory, outside the protective layer covering the integrated circuit and connected to the integrated circuit via the at least one terminal contact extending through the protective layer, and connected to the encryption unit of the integrated circuit via a data bus extending through the at least one terminal contact, the external second memory storing data encrypted with the cryptographic key stored in the first memory, wherein the encryption unit is designed to read data or code out of the external second memory, decrypt the data or code using the cryptographic key stored in the first memory, and write the**

decrypted data or code into the first memory or other memory of the integrated circuit. (See Kömmerling column 5 lines 45-50 "The encryption/decryption unit 120 operates to encrypt and decrypt using an encryption key 160 provided from a cryptographic input unit 130. The cryptographic input unit 130 is operative to form the key 160 from a plurality of detected property outputs 140 of a corresponding plurality of sensors 150 which are responsive to the encapsulation properties 170 of an encapsulation 50 surrounding the circuit.")

Kömmerling discloses an integrated circuit device with anti-tamper encapsulation, so when tampering with the encapsulation to gain access to the circuit causes the encryption and/or decryption to fail. (See Kömmerling abstract). Kömmerling does not explicitly disclose the limitation of "**a security sensor system including a protective layer covering the integrated circuit and a monitoring system that monitors the state of the protective layer covering the integrated circuit such that when a particular state of the protective layer is detected"** ; however, Mizuno discloses as claimed (see Mizuno page 15 lines 5-22 for original Japanese description, for translation purposes as stated above, the corresponding translation is equivalent to US 2004/0212017 A1) for [0096] of sixth embodiment "plural processing detector circuits 20 are dispersed irregularly within the main surface of the chip 3, whereby it is possible to make it difficult to identify the positions of the processing detector circuits 20 in the chip 3. In this regard, for analyzing information stored in the chip 3, it is conceivable that, after destroying the processing detector circuits 20, the foregoing wiring lines which function as a shield can be removed, followed by analysis of information stored in the

chip 3. Therefore, if plural processing detector circuits 20 are arranged in an irregularly dispersed fashion, it becomes difficult to destroy all of the processing detector circuits, and, hence, it is possible to make the analysis of information difficult. As a result, it becomes possible to further improve the security of information stored in the chip 3. Once the wiring lines 5A and 5B for the supply voltage are subjected to processing (complete or partial cutting), the processing detector circuits 20 are able to detect a change in potential (or resistance) of the wiring lines 5A and 5B. That is, the processing detector circuits 20 are used for the detection of tampering with the wiring lines 5A and 5B.")

Mizuno, similar to Kömmerling, is in the same field of endeavor of anti-tampering for semiconductors device, discloses the sensor and monitoring as claimed limitation for protection of the breaking of the wiring lines. (See Mizuno abstract)

Therefore, it would have been obvious to one of the ordinary skill in the art to use Mizuno in the invention of Kömmerling to include "the sensor and monitoring of a protective layer (e.g. resistance value of wiring changed) " as taught by Mizuno in order to improve the security of the IC for further protection for the circuit. (See Mizuno [0179-0183])

10. Claims 15, 17 and 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kömmerling and Mizuno as applied to claims 1 above, further in view of Candelore (US 5,861,662) hereinafter Candelore.

As for claim 15:

The combination of Kömmerling and Mizuno discloses **the arrangement comprising an integrated circuit as claimed claim 14,** neither Kömmerling nor Mizuno discloses **wherein the second memory is volatile and is connected to a battery so that the voltage supply is maintained when another power supply is lacking.** However, Candelore discloses as claimed. (See Candelore column 5 lines 49-55 "If an electrically conductive member is used in a component which did not have a battery powered erasure feature, then the electrically conductive member may instead carry various control signals.")

Candelore, like Kömmerling and Mizuno, is in the same field of endeavor of anti-tampering for semiconductors device, discloses the battery power for voltage supply when another power is lacking.

Therefore, it would have been obvious to one of the ordinary skill in the art to use Candelore in the modified-invention of Kömmerling to include the battery power as voltage supply so to improve the security of the IC for further protection for the circuit.

As for claim 17:

The combination of Kömmerling and Mizuno discloses **the arrangement comprising an integrated circuit as claimed claim 1,** neither Kömmerling nor Mizuno discloses **wherein the security sensor system is connected to a battery so that the voltage supply is maintained if another power supply is lacking.** However, Candelore discloses as claimed. (See Candelore column 2 lines 59-61" This signal may include a steady state electrical current which is supplied by a battery via positive and negative terminals. The wire may be carried, at least in part, in a protective layer of the IC such

that removal of the protective layer will rupture the wire, thereby causing an open circuit. ")

Candelore, like Kömmerling and Mizuno, is in the same field of endeavor of anti-tampering for semiconductors device, discloses the battery power for voltage supply when another power is lacking.

Therefore, it would have been obvious to one of the ordinary skill in the art to use Candelore in the modified-invention of Kömmerling to include the battery power as voltage supply so to improve the security of the IC for further protection for the circuit.

As for claim 18:

The combination of Kömmerling and Mizuno discloses **the arrangement comprising an integrated circuit as claimed claim 1;** neither Kömmerling nor Mizuno discloses **wherein the security sensor system is connected to an auxiliary power source, integrated in the package, which provides the power for deleting the first memory.** However, Candelore discloses as claimed. (see Candelore column 1 lines 50-60 "If the chip requires a direct current from a battery or the like to circumvent a self-destruct feature, then battery wires are soldered to a positive voltage pin (e.g., V_{batt}) pin and to a negative voltage pin (e.g., V_{ss}) on the outside of the chip prior to removal from the board.") Candelore discloses the battery as an auxiliary power source.

Candelore, like Kömmerling and Mizuno, is in the same field of endeavor of anti-tampering for semiconductors device, discloses the battery power providing the power.

Therefore, it would have been obvious to one of the ordinary skill in the art to use Candelore in the modified-invention of Kömmerling to include the battery power as

providing auxiliary power source so to improve the security of the IC for further protection for the circuit.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this office action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to JASON LEE whose telephone number is (571)270-7477. The examiner can normally be reached on Monday-Friday 9/5/4 (altering Friday off).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Taghi T Arani can be reached on (571)272-3787. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/J. L./
Examiner, Art Unit 2438
/Taghi T. Arani/

Supervisory Patent Examiner, Art Unit 2438